DIGITAL SOVEREIGNTY

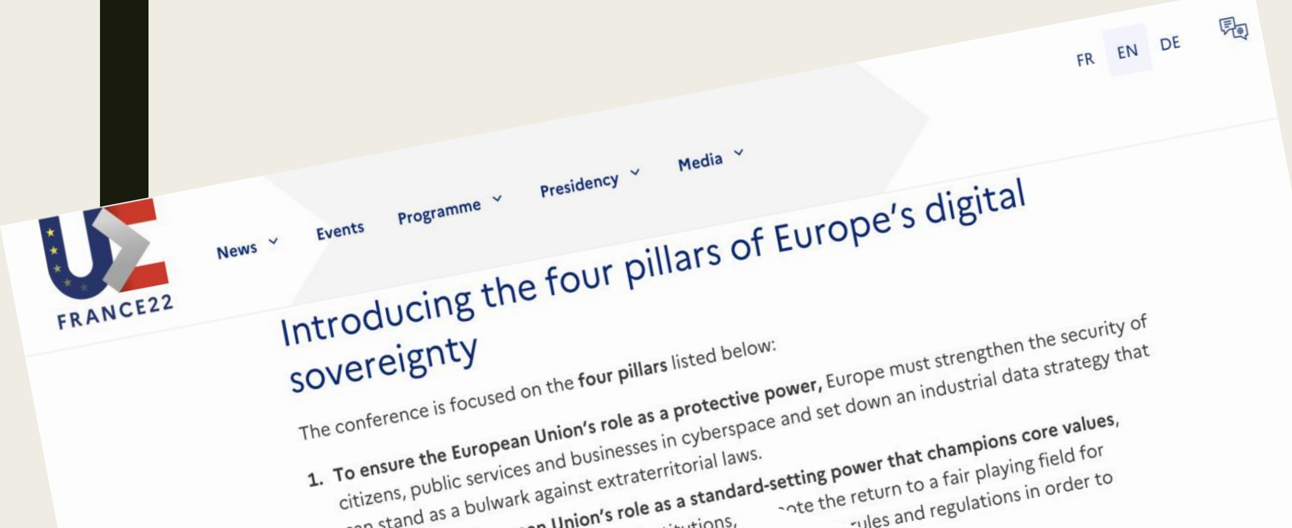
Mireille Hildebrandt, FBA
Professor of law

Faculty of Law & Criminology, Vrije Universiteit Brussel
Faculty of Science, Radboud University

Preliminary observations

- Effective and practical protection of fundamental rights
- Depends on there being a state/jurisdiction with an independent court
- In other words: **no sovereignty no legal protection**
- Though this does not imply that all sovereign states offer such protection

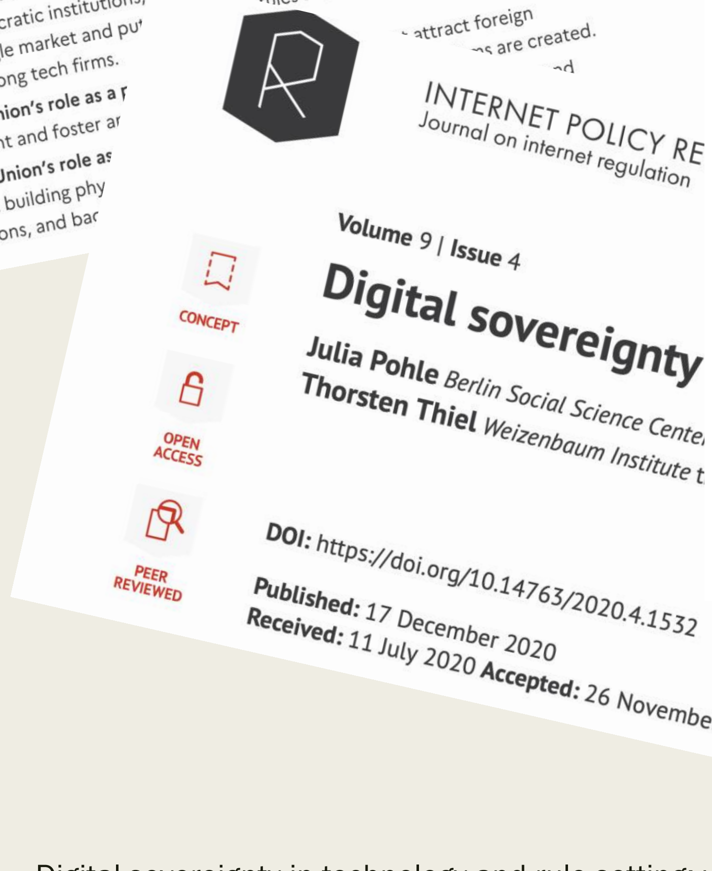
- Things that matter are incomputable
- But they can be made computable
- **They can be made computable in different ways, and those difference matter**



Introducing the four pillars of Europe's digital sovereignty

The conference is focused on the **four pillars** listed below:

1. **To ensure the European Union's role as a protective power,** Europe must strengthen the security of citizens, public services and businesses in cyberspace and set down an industrial data strategy that can stand as a bulwark against extraterritorial laws.
2. **To ensure the European Union's role as a standard-setting power that champions core values,** Europe must shore up democratic institutions, ote the return to a fair playing field for businesses in the digital single market and pu rules and regulations in order to increase accountability among tech firms.
3. **To ensure the European Union's role as a r** attract foreign investors and foreign talent and foster ar s are created.
4. **To ensure the European Union's role as** nd open standards, support building phy the global digital commons, and bac



Volume 9 | Issue 4

Digital sovereignty

Julia Pohle Berlin Social Science Cente

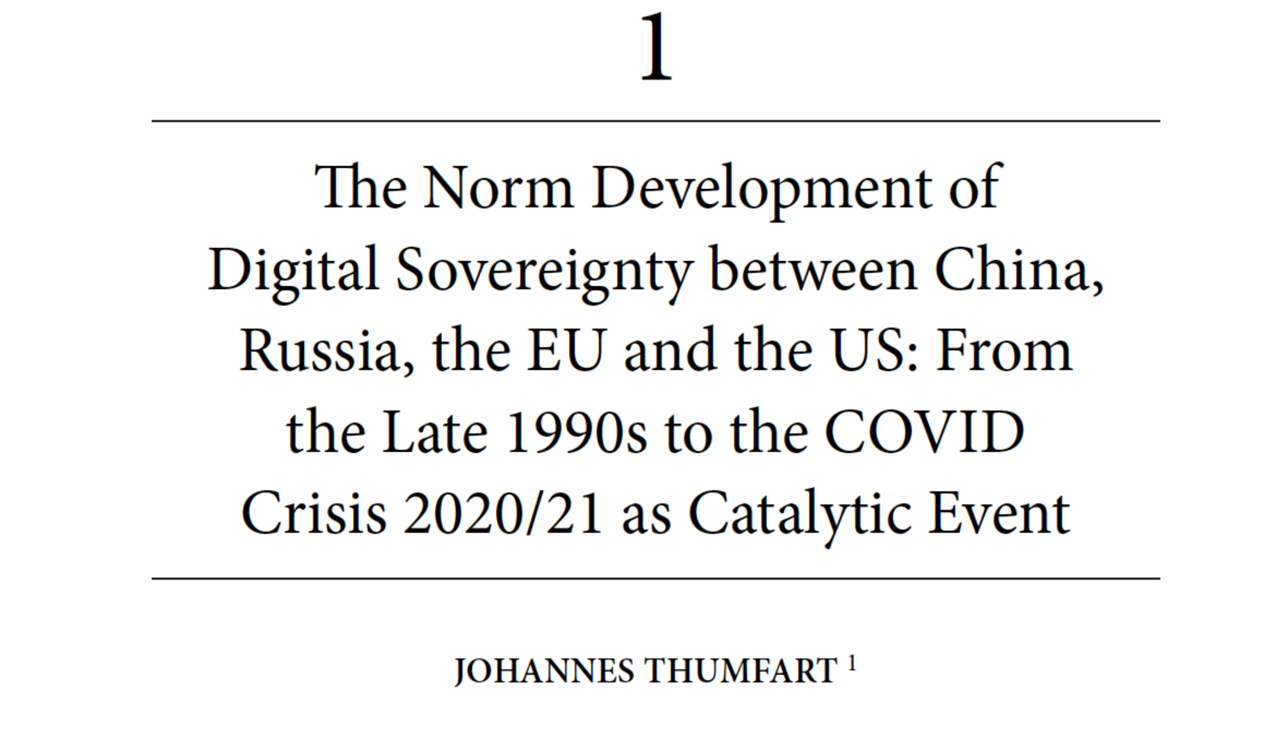
Thorsten Thiel Weizenbaum Institute t

DOI: https://doi.org/10.14763/2020.4.1532

Published: 17 December 2020

Received: 11 July 2020 **Accepted:** 26 November 2020

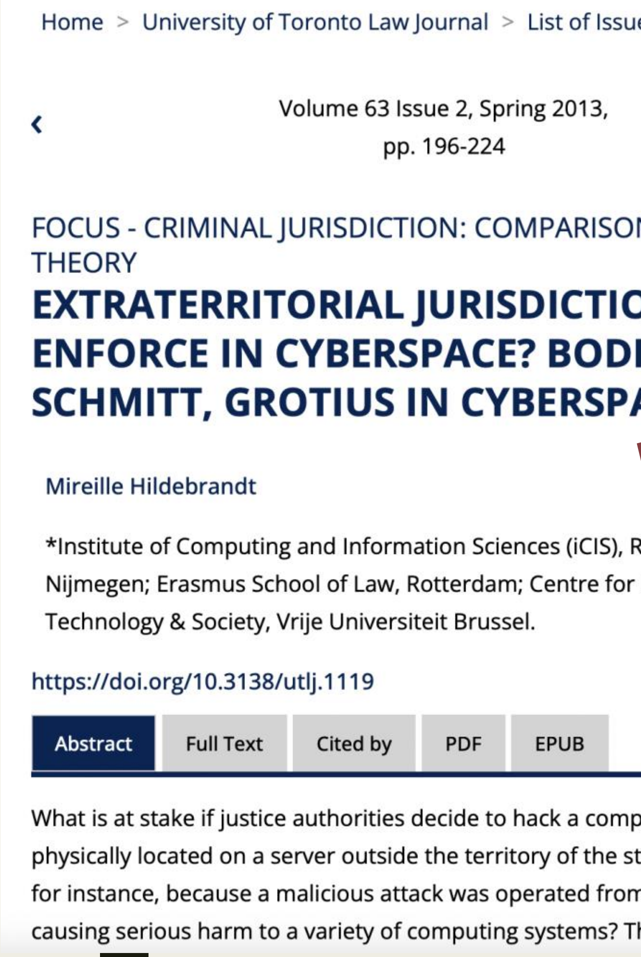
Johannes Thumfart, 'The Norm Development of Digital Sovereignty between China, Russia, the EU and the US: From the Late 1990s to the Covid-Crisis 2020/21 as Catalytic Event', in Enforcing Rights in a Changing World, ed. Dara Hallinan, Ronald Leenes, and Paul de Hert, Computers Privacy Data Protection (CPDP) 14 (London: Hart Publishing, 2022), 1–44.



1

The Norm Development of Digital Sovereignty between China, Russia, the EU and the US: From the Late 1990s to the COVID Crisis 2020/21 as Catalytic Event

JOHANNES THUMFART [1]



Home > University of Toronto Law Journal > List of Issues > Vol. 63, No. 2 > D

Volume 63 Issue 2, Spring 2013,
pp. 196-224

FOCUS - CRIMINAL JURISDICTION: COMPARISON, HISTORY, THEORY

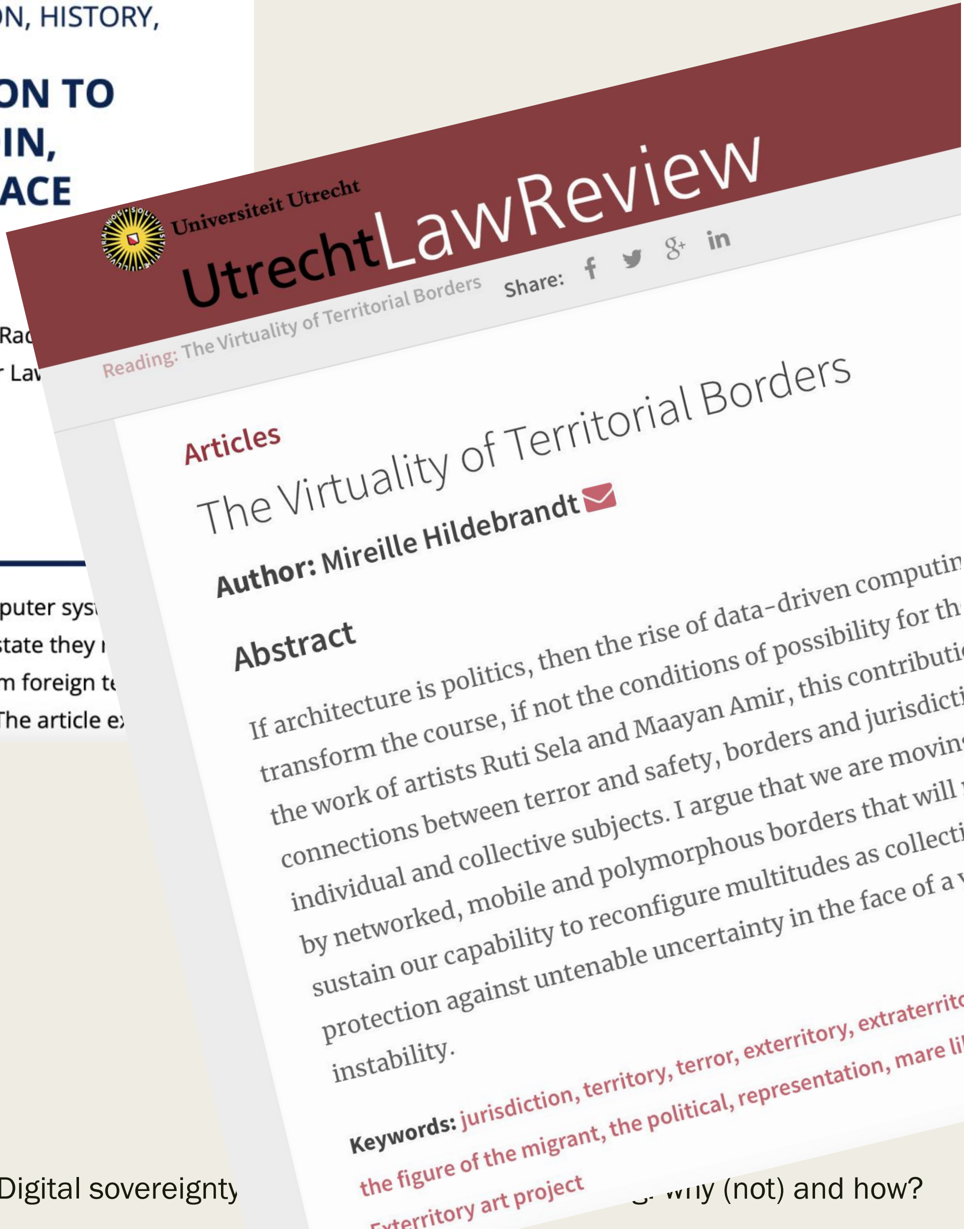
EXTRATERRITORIAL JURISDICTION TO ENFORCE IN CYBERSPACE? BODIN, SCHMITT, GROTIUS IN CYBERSPACE

Mireille Hildebrandt

*Institute of Computing and Information Sciences (iCIS), Rad
Nijmegen; Erasmus School of Law, Rotterdam; Centre for Law
Technology & Society, Vrije Universiteit Brussel.

https://doi.org/10.3138/utlj.1119

What is at stake if justice authorities decide to hack a computer syst
physically located on a server outside the territory of the state they r
for instance, because a malicious attack was operated from foreign te
causing serious harm to a variety of computing systems? The article ex



Articles

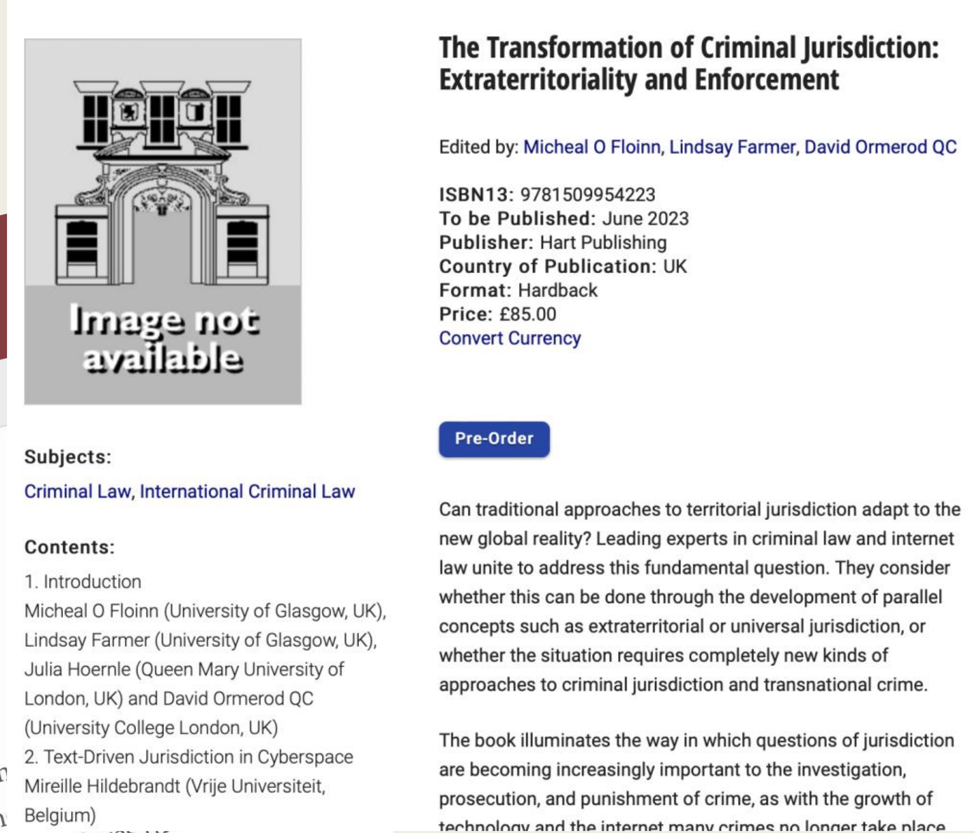
The Virtuality of Territorial Borders

Author: Mireille Hildebrandt

Abstract

If architecture is politics, then the rise of data-driven computin
transform the course, if not the conditions of possibility for th
the work of artists Ruti Sela and Maayan Amir, this contribution explores th
connections between terror and safety, borders and jurisdictions, and those between
individual and collective subjects. I argue that we are moving into a world constituted
by networked, mobile and polymorphous borders that will require hard work to
sustain our capability to reconfigure multitudes as collective subjects, offering
protection against untenable uncertainty in the face of a volatile jurisdictional
instability.

Keywords: jurisdiction, territory, terror, exterritory, extraterritorial, cyberspace, virtual, actual, the figure of the migrant, the political, representation, mare liberum, cyberspace liberum, Exterritory art project



The Transformation of Criminal Jurisdiction: Extraterritoriality and Enforcement

Edited by: Micheal O Floinn, Lindsay Farmer, David Ormerod QC

ISBN13: 9781509954223
To be Published: June 2023
Publisher: Hart Publishing
Country of Publication: UK
Format: Hardback
Price: £85.00
Convert Currency

Subjects:
Criminal Law, International Criminal Law

Contents:

Can traditional approaches to territorial jurisdiction adapt to the new global reality? Leading experts in criminal law and internet law unite to address this fundamental question. They consider whether this can be done through the development of parallel concepts such as extraterritorial or universal jurisdiction, or whether the situation requires completely new kinds of approaches to criminal jurisdiction and transnational crime.

The book illuminates the way in which questions of jurisdiction are becoming increasingly important to the investigation, prosecution, and punishment of crime, as with the growth of technology and the internet many crimes no longer take place

What's next?

- Conceptual exploration: sovereignty
- Digital sovereignty: software and hardware
- Geopolitical interdependence: bug or feature
- Rule-setting: why (not) and how?

What's next?

- Conceptual exploration: sovereignty
- Digital sovereignty: software and hardware
- Geopolitical interdependence: bug or feature
- Rule-setting: why (not) and how?

sovereignty

- Rise of the (proto)state:
  - Conscription and taxes
  - Military and political power
- Sovereignty:
  - The power to command over a people and/or a territory
  - The concept first appeared in 14th century France
  - The concept was ‘defined’ by Bodin in the 16th century
    - absolute centralised power to develop and sustain the ***res publica***
    - ***not having to negotiate*** with powerful players about the res publica

sovereignty

- Rise of the modern state
- Concepts of ***territory*** and ***jurisdiction***
  - ‘Jurisdiction’ early 14th century,
    - initially referring to the administration of justice
    - and soon meaning ‘extent or range of administrative power’.
  - ‘Territory’ early 15th century
    - then meaning ‘land under the jurisdiction of a town, state, etc.’

sovereignty

- Rise of the modern state
- Concepts of ***territory*** and ***jurisdiction***
  - Territorial jurisdiction
    - ***Terroir*** (land)
    - ***Terror*** (capable of terrorising those outside and those inside)
    - Note the connection with ***the monopoly of violence* and *internal and external sovereignty***

sovereignty

- 1648 Peace of Westphalia
  - Rise of international law as constitutive of
    - Internal and external sovereignty
    - ‘gleichursprünglich’ or ‘mutually constitutive’
  - National law made possible by international law
  - International law made possible by national law

sovereignty

- The international legal order assumes
  - Mutually exclusive territorial jurisdictions
  - Where a sovereign rules over a territory and those/that within its borders
  - No land without a state, no state without land
  - Contiguous mapping of the land of the world

sovereignty

- This was enabled by two ***technologies***:
  - Cartography and the printing press

note that this is not about technological determinism

sovereignty

- **The invention of cartography** (Richard Ford):
  1. authority is to be exercised primarily ***by area***, instead of status or family
  2. ***territorial boundaries*** are not ambiguous or contested (except in times of crisis or transition)
  3. jurisdiction refers to an ***'abstract space'*** that 'reduces space to an empty vessel for government power.'
  4. cartographic mapping produces a '***"gapless" map of contiguous political territories***, thus grounding the Westphalian system of mutually exclusive territorial jurisdictions'.
- This notion of jurisdiction is ***constructive/artificial*** (Ford, Tönnies):
  - Not dependent on organically grown *Gemeinschaft*
  - Affording the development of an instituted *Gesellschaft*
- Reminding us of Hobsbawn's *The Invention of Tradition*

sovereignty

- **The proliferation of the printing press** (Hildebrandt):
  - This is about ICT *infrastructure*
  - Affordances of the technologies of the word (Ong, Eisenstein, Goody, Ricoeur):
    - Distantiation between author and text, author and reader, text and meaning
    - Enlarging the scope of the audience in time and space
    - Requiring increasing systematisation (structuring, indexing, mapping, storing)
- Turning jurisdiction into an abstract space ruled by way of primary and secondary rules:
  - The legislature as author, civil servants as readers/enforcers of the law
  - Those sharing jurisdiction as readers/subject to the law
  - Role of legal certainty, recognizing the ability to change the law
  - Interpretation and argumentation become the hallmarks of the law

sovereignty

- Jellinek about ‘*Die normative Kraft des Faktischen*’ in elements of statehood:
  - People
  - Territory
  - Political power (validity, effectiveness)
- Complemented with
  - Recognition (limits to self determination, connection with political power)
  - 1933 Montevideo Convention on Rights and Duties of States

sovereignty

What about democracy and the rule of law?

- Protection of constitutional democracies requires territorial jurisdiction
- Legal protection of fundamental rights assumes sovereignty:
  - An effective monopoly of violence
  - Without ‘unilateral jurisdiction to enforce’ no protection
- Rule of law (Rechtsstaat) is contingent upon sovereignty
  - it concerns the internal division of powers (Montesquieu)
  - without such sovereignty there is nothing to divide

What's next?

- Conceptual exploration: sovereignty
- Digital sovereignty: software and hardware
- Geopolitical interdependence: bug or feature
- Rule-setting: why (not) and how?

Digital sovereignty

- Is digital sovereignty about nationalist or EU protectionism?
- Is digital sovereignty about protection of natural persons in dxigital contexts?
- What is the role of territorial sovereignty here?

Digital sovereignty

- Digital technologies set rules
  - They invite/inhibit or even enforce/preclude specific behaviours
- What rules they set depends on a series of **upstream design decisions**
  - Made by those who invest in their development and those who develop the techs
- What rules they set also depends on **downstream design/interface/deployment decisions**
  - The effect of all these decisions does not necessarily depend on intent
- **Legal Protection by Design** means
  - Legal rules to reset technological rules, aiming for rule-of-law checks and balances

Digital sovereignty

- Sovereignty as we know it is territorial

Digital sovereignty

- ‘Digital sovereignty’ is a misnomer
  - it is always about ***territorial sovereigns***
  - aiming to gain control over
  - transnational digital infrastructure and data flows

Digital sovereignty

- Transnational digital infrastructure and data flows:
    - Hardware, software and data, but also protocols and standards

Digital sovereignty

- Hardware (global cloud, mobile and transnational smart grid infrastructure, cables, servers, satellites, chips, connected vehicles, IoT)
  - Who owns the hardware, who controls the hardware?
  - Who can access the systems/data that depend/run on the hardware?
  - How to protect those within a territorial jurisdiction:
    - Their safety
    - Their fundamental rights (both freedom from and freedom to)
  - How does this relate to self determination (of individuals, of jurisdictions)

Digital sovereignty

- Software (global tech platforms, social media, online gaming, VR, metaverses, recommender systems, search engines, AI systems including medical, educational, automated pilots, tax and social benefits, smart policing and IoT cyberphysical infrastructure)
  - General AI systems, such as FR and NLP (autocomplete)
  - Running of AI systems in cloud infrastructure
  - How to protect those within a territorial jurisdiction?
    - Their safety
    - Their fundamental rights
  - How does this relate to self determination (of individuals and jurisdictions)?

Digital sovereignty

- Data (behavioural, location and mobility, public health related, energy usage, IP & trade secret protected, IoT cyberphysical infrastructure data flows)
  - Access to training data, quality issues
    - Data = a proxy (ground truth is always a proxy)
    - Concept drift and data drift: data by default lagging behind
    - Most data ‘sits’ in public clouds owned by private companies
  - How to protect those within a territorial jurisdiction?
    - Their safety
    - Their fundamental rights
  - How does this relate to self determination (of individuals and jurisdictions)?

Digital sovereignty

- Protocols (TCP/IP and HTTP) and standards (ISO, IEEE), including those for software, requirements engineering, AI and IoT
  - Who defines the protocols and the standards?
  - Which players: vendors, governments, developers etc?
  - What geo-political implications?
    - China/India: neo-colonial reign
  - How to protect those within a territorial jurisdiction?
    - Their safety
    - Their fundamental rights
  - How does this relate to self determination (of individuals and jurisdictions)?

Digital sovereignty

- Digital sovereignty is a norm (Thumfart)
  - on how to sustain
  - both internal and external sovereignty
  - US vs China vs EU
- Concept of DS originated in China and Russia:
  - against neo-colonial and neo-imperial global reign

Digital sovereignty

- States versus VLOPs
  - remember Bodin:
    - a sovereign that has to negotiate with big players is a feudal suzereign

What's next?

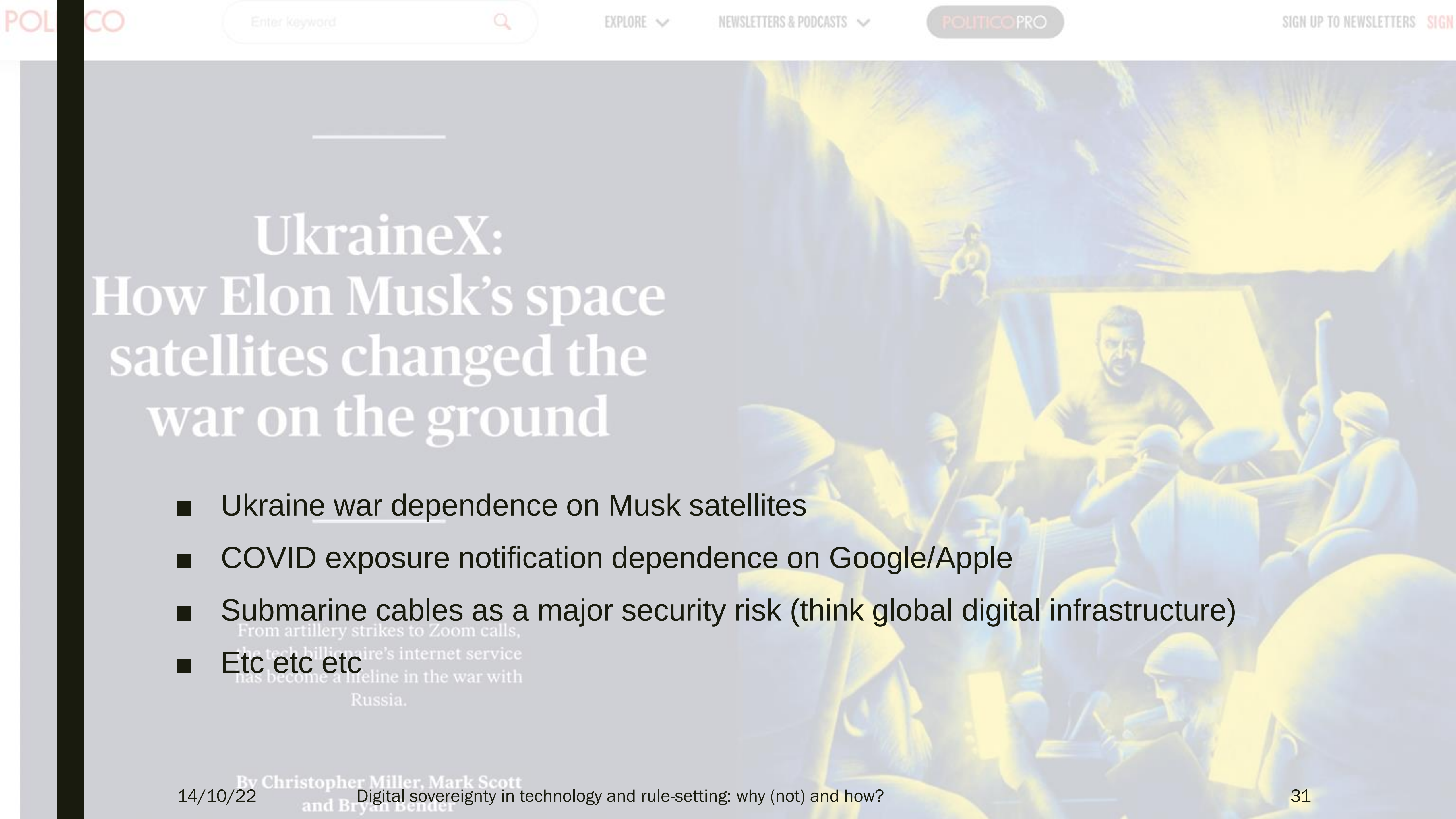
- Conceptual exploration: sovereignty
- Digital sovereignty: software and hardware
- **Geopolitical interdependence: bug or feature**
- Rule-setting: why (not) and how?

Digital sovereignty

Digital transformation and the geopolitical arms race:

- Google, Amazon, Facebook, Apple and Microsoft (GAFAM) in the US
- Baidu, Alibaba, Tencent and Huawei (BATH) in China

  - My position is that the EU should not buy into the rethorics of an arms race,
    - But no reason for complacency

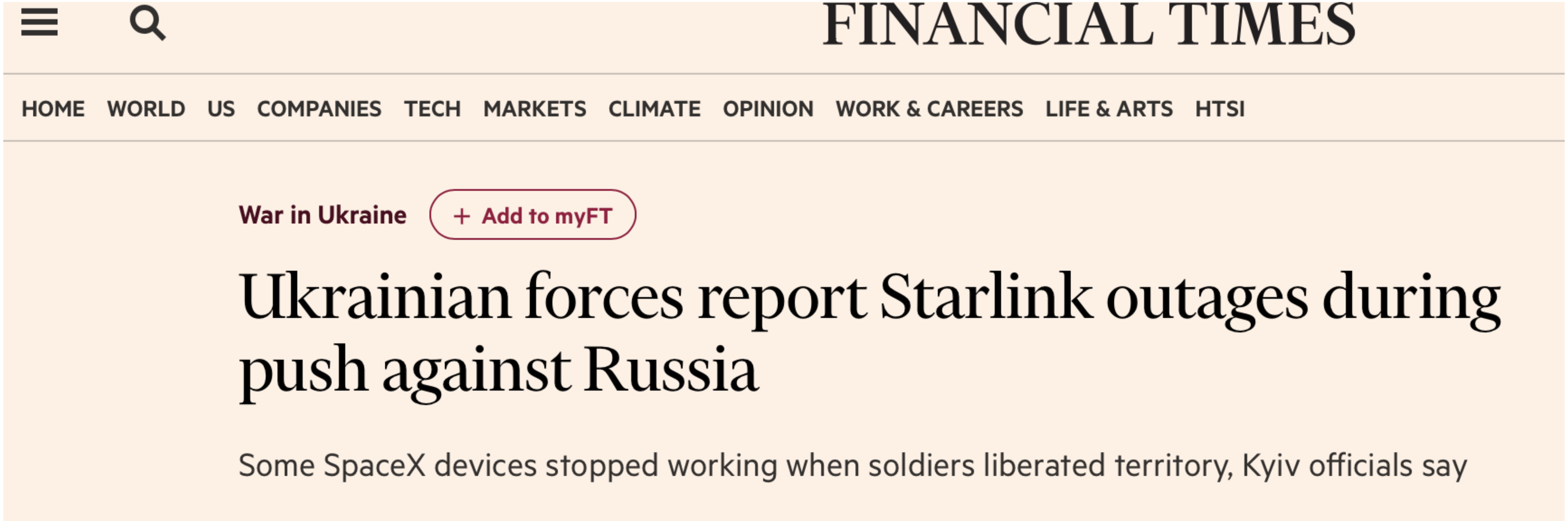


UkraineX: How Elon Musk's space satellites changed the war on the ground

From artillery strikes to Zoom calls, the tech billionaire's internet service has become a lifeline in the war with Russia.

By Christopher Miller, Mark Scott and Bryan Bender

- Ukraine war dependence on Musk satellites
- COVID exposure notification dependence on Google/Apple
- Submarine cables as a major security risk (think global digital infrastructure)
- Etc etc etc



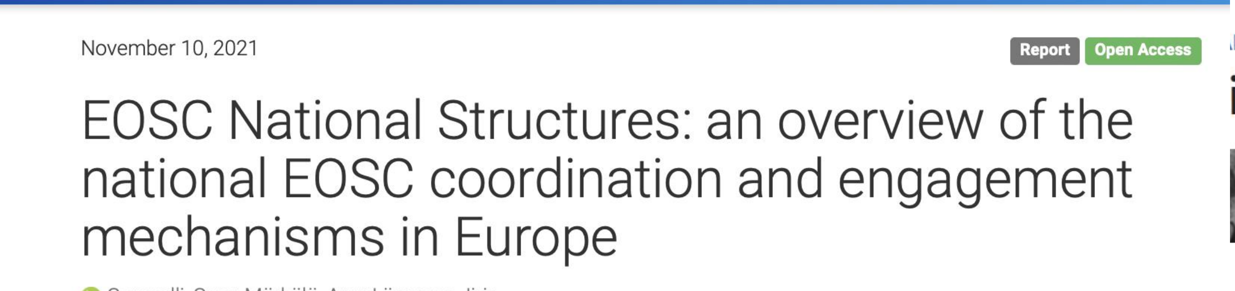
Ukrainian forces report Starlink outages during push against Russia

Some SpaceX devices stopped working when soldiers liberated territory, Kyiv officials say

Digital sovereignty

- Let’s focus on cloud infrastructure for a minute,
  as an enabler of ‘the digital transformation’:
  AI development and deployment,
  notably search, FR, NLP, and
  big data storage
- plus – major contribution to climate change

(Not saying other hardware, software, data, protocols and standards deserve less attention)



November 10, 2021

Report Open Access

EOSC National Structures: an overview of the national EOSC coordination and engagement mechanisms in Europe

Garavelli, Sara; Märkälä, Anu; Liinamaa, Iiris

The European Open Science Cloud (EOSC) Partnership **will bring together institutional, national and Eur** and engage all relevant stakeholders to **co-design and deploy a European Research Data C**

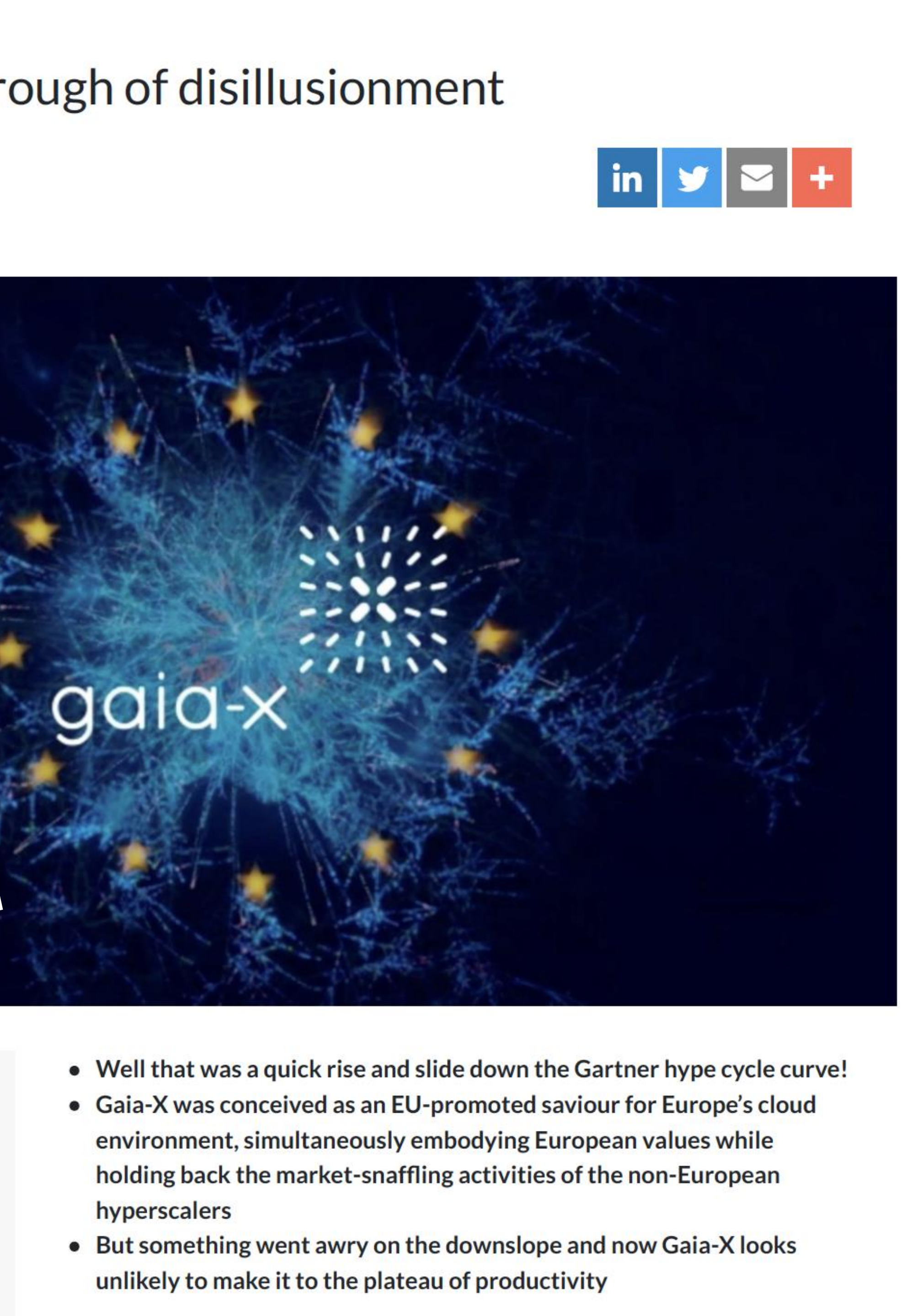
The Partnership will seek engagement with the Member States and A Board" external to the EOSC Association; ii) and via me

In addition to these official enga with the **goal of c**

Cecilia Rikap · Bengt-Åke Lundvall

The Digital Innovation Race

Conceptualizing the Emerging New World Order



L PLATFORMS & SERVICES

ia-X hits the trough of disillusionment

By Ian Scales
Oct 7, 2022

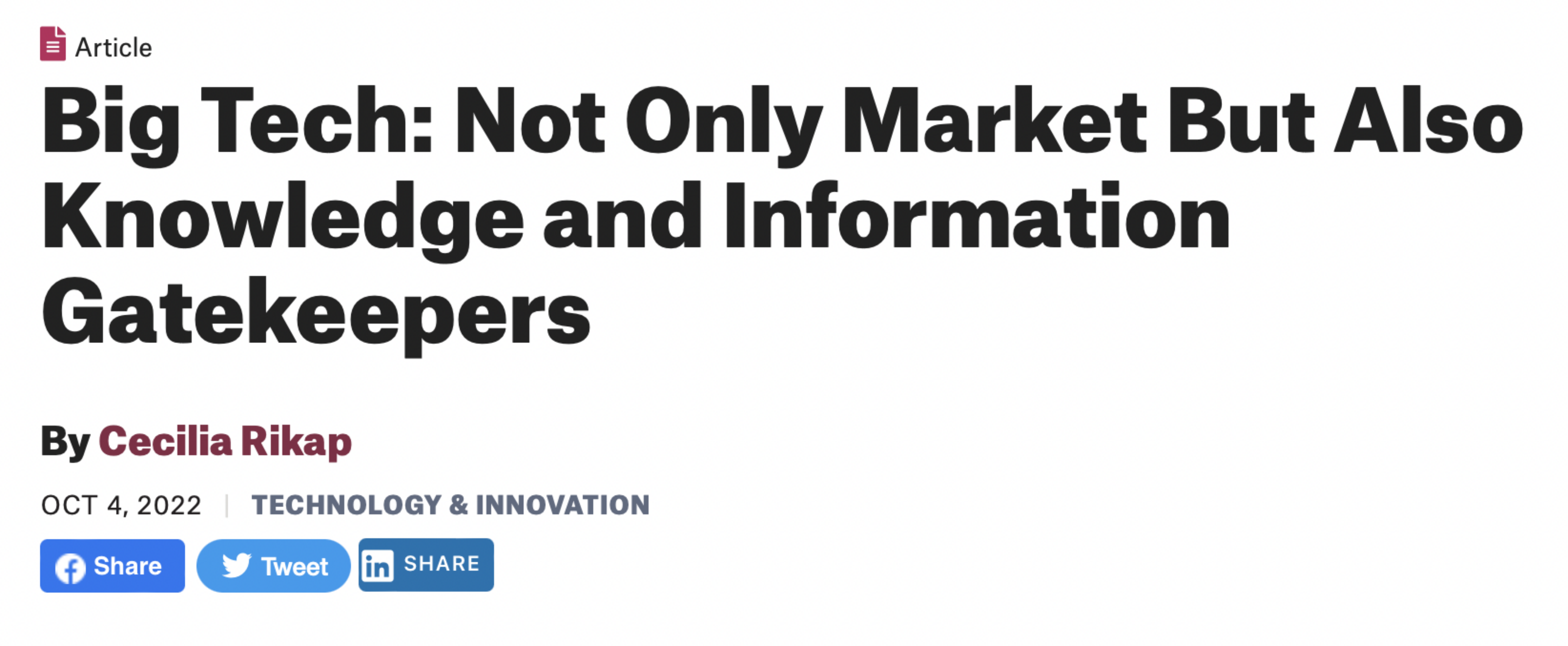
Related Topics

Analysis & Opinion, Cloud, Digital Platforms & Services, Enterprise, Europe, News

More Like This

DIGITAL PLATFORMS & SERVICES

- Well that was a quick rise and slide down the Gartner hype cycle curve!
- Gaia-X was conceived as an EU-promoted saviour for Europe's cloud environment, simultaneously embodying European values while holding back the market-snaffling activities of the non-European hyperscalers
- But something went awry on the downslope and now Gaia-X looks unlikely to make it to the plateau of productivity



Article

Big Tech: Not Only Market But Also Knowledge and Information Gatekeepers

By Cecilia Rikap

OCT 4, 2022 | TECHNOLOGY & INNOVATION

Digital sovereignty

Cloud infrastructure

- 2012: firms spent 6.5b USD on cloud infrastructure services
- 2021: 178b USD (an increase of 2.638%)
- ownership Amazon, Microsoft and Google 65%

- development and deployment of AI applications depends on cloud infrastructure:
  - big data to train AI models
  - running general AI systems (FR or NLP)

Digital sovereignty

Cloud infrastructure

- EU:
  - GAIA-X (public-private)
    - Integrating US big tech cloud providers?
  - EOSC (public, what cloud providers?)
    - Collaborative framework, enabling federated learning etc.
  - EU Data spaces DGA, notably the EHDS (public, what cloud providers?)
  - Siemens (private)
    - MindSphere, a cloud platform for storing and analyzing data retrieved with IoT from its sold equipment
    - AWS took over part of this platform's development, providing computing services that Siemens cannot develop in-house and requires to provide AI-specific solutions to its clients

Digital sovereignty

Cloud infrastructure

- EU Commission approves acquisition of Nuance by Microsoft:
  - Nuance, a cloud-based system for medical transcription services, acquired for USD 19.7 billion
  - MS thus gains a strong foothold in cloud services for the healthcare industry, a source of colossal datasets to be exploited with artificial intelligence.

- Remember the involvement of Palantir in NHS (UK) and many EU states during the pandemic
- Try to imagine who will have access to our health data
  as a way to commodify health data to extract a surplus

Digital sovereignty

Cloud infrastructure

- EU:
  - cloud computing offers technology as a black box
  - it limits users’ learning and generates a form of long-term technological dependence with no visible ways of moving beyond it.
  - tech giants’ algorithms selfimprove by processing the data harvested by companies like Siemens, thus further expanding the technological gap between cloud providers and other firms

What's next?

- Conceptual exploration: sovereignty
- Digital sovereignty: software and hardware
- Geopolitical interdependence: bug or feature
- Rule-setting: why (not) and how?

Rule-setting: why (not) and how?

- Digital technologies set rules
  - They invite/inhibit or even enforce/preclude specific behaviours
- What rules they set depends on a series of **upstream design decisions**
  - Made by those who invest in their development and those who develop the techs
- What rules they set also depends on **downstream design/interface/deployment decisions**
  - The effect of all these decisions does not necessarily depend on intent
- **Legal Protection by Design** means
  - Legal rules to reset technological rules, aiming for rule-of-law checks and balances

Rule-setting: why (not) and how?

The political economy that is generated, reinforced or enabled by big tech platforms

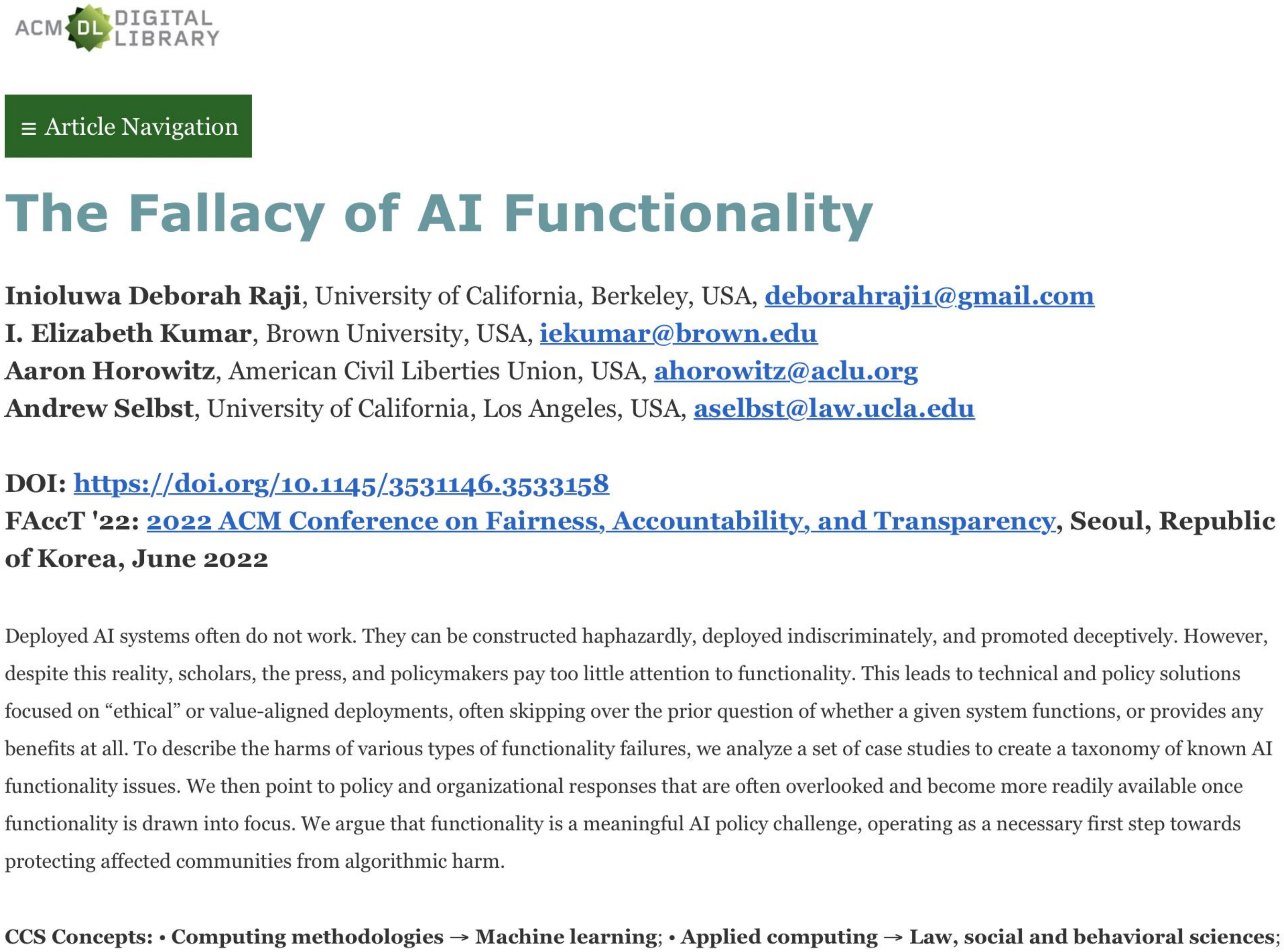
- ‘Natural’ monopolies and monopsonies, concentration of power
- Network effects, path dependency
- Major power imbalances:
  - Between consumers and those who micro-target them (invisible visibility)
  - Between employees/geek workers and those who micro-target them (algorithmic manipulation, invisible visibility, automation bias)
  - Between cloud providers and social networks - and other firms (who actually make something)

Rule-setting: why (not) and how?

- GDPR and LED (ePrivacy directive etc.)
- Representative directive
- DMA, DSA, DGA, DA, AI Act, AI Liability Directive
- Copyright and Trade Secret legislation

Rule-setting: why (not) and how?

- Smuha:
  - The arms race to get AI regulation right
- Bradford:
  - The Brussels effect



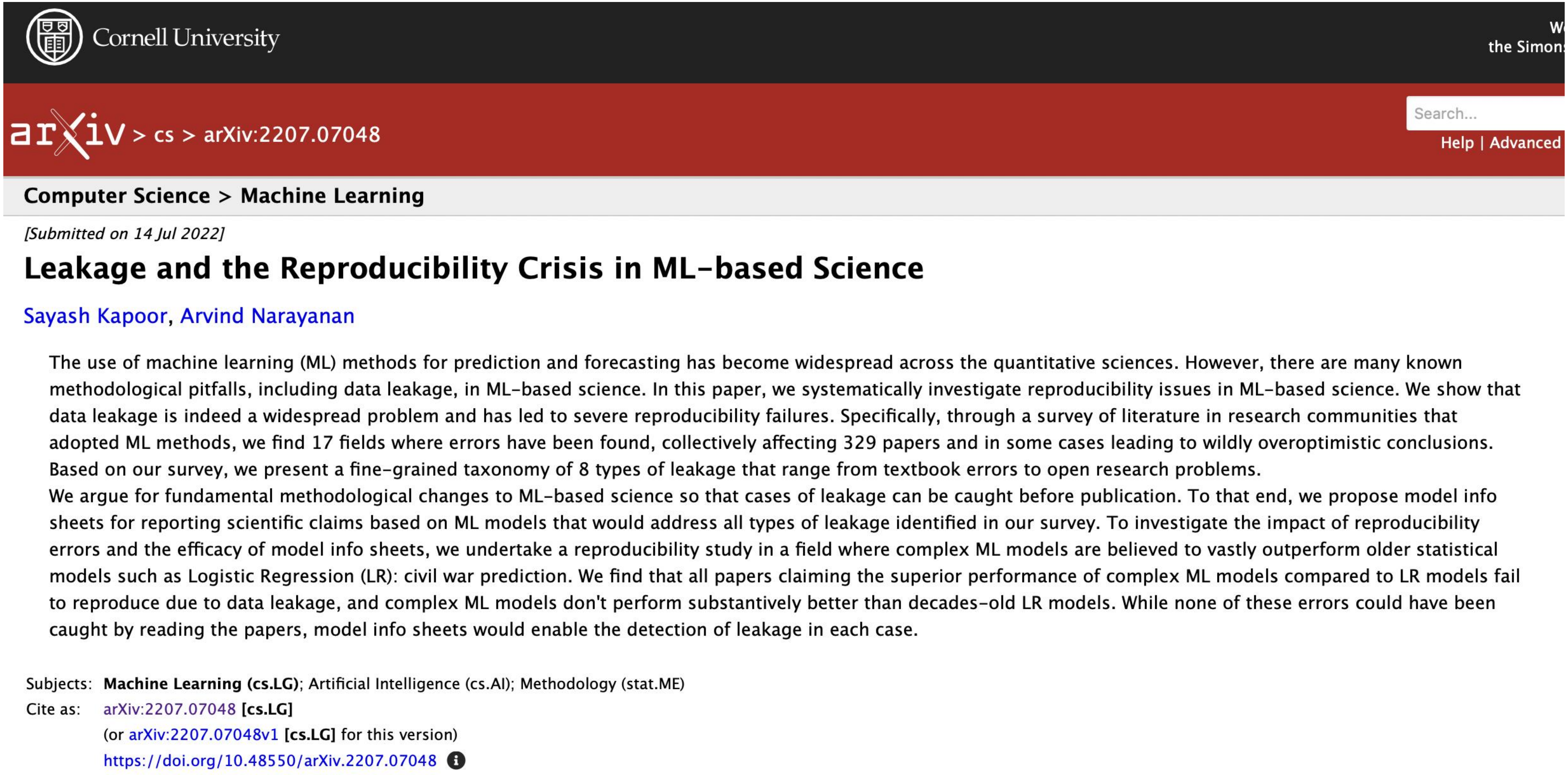
The Fallacy of AI Functionality

Inioluwa Deborah Raji, University of California, Berkeley, USA, deborahraji1@gmail.com
I. Elizabeth Kumar, Brown University, USA, iekumar@brown.edu
Aaron Horowitz, American Civil Liberties Union, USA, ahorowitz@aclu.org
Andrew Selbst, University of California, Los Angeles, USA, aselbst@law.ucla.edu

DOI: https://doi.org/10.1145/3531146.3533158
FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency, Seoul, Republic of Korea, June 2022

Deployed AI systems often do not work. They can be constructed haphazardly, deployed indiscriminately, and promoted deceptively. However, despite this reality, scholars, the press, and policymakers pay too little attention to functionality. This leads to technical and policy solutions focused on “ethical” or value-aligned deployments, often skipping over the prior question of whether a given system functions, or provides any benefits at all. To describe the harms of various types of functionality failures, we analyze a set of case studies to create a taxonomy of known AI functionality issues. We then point to policy and organizational responses that are often overlooked and become more readily available once functionality is drawn into focus. We argue that functionality is a meaningful AI policy challenge, operating as a necessary first step towards protecting affected communities from algorithmic harm.

CCS Concepts: • Computing methodologies → Machine learning; **• Applied computing → Law, social and behavioral sciences**;


Cornell University
W
the Simon
arXiv > cs > arXiv:2207.07048
Search...
Help | Advanced
Computer Science > Machine Learning

[Submitted on 14 Jul 2022]

Leakage and the Reproducibility Crisis in ML-based Science

Sayash Kapoor, Arvind Narayanan

The use of machine learning (ML) methods for prediction and forecasting has become widespread across the quantitative sciences. However, there are many known methodological pitfalls, including data leakage, in ML-based science. In this paper, we systematically investigate reproducibility issues in ML-based science. We show that data leakage is indeed a widespread problem and has led to severe reproducibility failures. Specifically, through a survey of literature in research communities that adopted ML methods, we find 17 fields where errors have been found, collectively affecting 329 papers and in some cases leading to wildly overoptimistic conclusions. Based on our survey, we present a fine-grained taxonomy of 8 types of leakage that range from textbook errors to open research problems.

We argue for fundamental methodological changes to ML-based science so that cases of leakage can be caught before publication. To that end, we propose model info sheets for reporting scientific claims based on ML models that would address all types of leakage identified in our survey. To investigate the impact of reproducibility errors and the efficacy of model info sheets, we undertake a reproducibility study in a field where complex ML models are believed to vastly outperform older statistical models such as Logistic Regression (LR): civil war prediction. We find that all papers claiming the superior performance of complex ML models compared to LR models fail to reproduce due to data leakage, and complex ML models don't perform substantively better than decades-old LR models. While none of these errors could have been caught by reading the papers, model info sheets would enable the detection of leakage in each case.

Subjects: **Machine Learning (cs.LG)**; Artificial Intelligence (cs.AI); Methodology (stat.ME)
Cite as: arXiv:2207.07048 **[cs.LG]**
(or arXiv:2207.07048v1 **[cs.LG]** for this version)
https://doi.org/10.48550/arXiv.2207.07048 ℹ

Rule-setting: why (not) and how?

- AI Act:
  - Accountability is mainly with those who put AI systems on the market
  - For high risk systems detailed reliability requirements
  - Risk management for intende purpose and reasonably foreseeable misuse
  - Human oversight when deployed
  - Conformity and auditability as to foreseeable fundamental rights infringements

Rule-setting: why (not) and how?

- Digital sovereignty:
  - we do not want unreliable, unsafe systems on the market that risk infringing fundamental rights
  - to some extent we will need to develop our own hardware/software/data/protocols/standards to safeguard such reliability, safety and effective respect for fundamental rights
  - to enable this we need **legislation to shape the internal economic market** such that it becomes conducive to this kind of technological design

- We need to think in terms of **Legal Protection by Design**
  not to be confused with ‘legal by design’ – ‘compliance/enforcement by design’

THE END IS NEAR
ACTUALLY, THIS IS JUST THE BEGINNING
m.E.mcnair